REMARKS

Reconsideration and allowance in view of the foregoing amendments and the following remarks are respectfully requested. By this Amendment, claim 22 has been canceled without prejudice. Claims 1-21, and 23-26 have been amended to merely clarify the recited invention without the intention of narrowing the scope of any of those claims. No new matter has been submitted as the claims are fully supported by the originally filed application. Upon entry of this Amendment, claims 1-21, 23-26 will be pending.

In Section 3 of the Office Action, dated November 4, 2002, the Examiner raised questions related to the interpretation of the transaction method recited in claim 1. The amended claim 1 clarifies the different aspects of the raised questions. The authorization data is stored in the terminal and used for checking the authorization of the customer. The authorization data can be periodically updated via a public switched telephone network, as recited in the amended claim 1. In addition, the authorization of the customer is checked before the terminal communicates with the service center. In addition, a transaction document is sent from the terminal to a service center after the terminal successfully verifies the authorization of the customer, as recited in the amended claim 1.

In Section 4 of the Office Action, an informality in the specification is objected to. The corresponding portion of the specification is accordingly amended to overcome the informality objection.

In Section 6 of the Office Action, the Examiner rejected claims 1-26 under 35 U.S.C. §112, first paragraph. The amended claims 1 and 12 clarify the Examiner's question related to the relationship between a mobile device and the terminal. The Examiner raised a question regarding where the specification provides support that the terminal checks the electronic signature of the identification module. Claim 5 is supported by the portion of the specification on page 11, lines 5-6, with reference to Figure 3, page 4, lines 18-22, and page

8, lines 9-13. To address the question raised by the Examiner regarding the support for claim 9, the support for "customer blocking documents" can be found on page 12, lines 23-27, with reference to Figure 1 and Figure 2. We further amended this paragraph to clarify the generation and the role of "terminal blocking documents".

In Section 8 of the Office Action, the Examiner rejected claims 1-26 under 35 U.S.C. §112, second paragraph. The amended claim 1 clarifies, in its body, the role of the mobile radio telephone in the claimed transaction method and its relationship with other parts during a transaction. In addition, claims 4, 9, 10, 14, 15, 19, 21, and 26 have been amended to clarify the recited questions.

In Section 10 of the Office Action, claims 1-12, 15-19, and 21-26 have been rejected under 35 U.S.C. § 103 (a) as being unpatentable over Vazvan (WO 97/45814), Vatanen (U.S. Patent No. 6,169,890), in view of Pitroda (U.S. Patent No. 5,590,038) and O'Mahony et al. Pieterse et al. Applicants respectfully traverse the rejection. The combination of Vazvan, Vatanen, Pitroda, and O'Mahony fails to teach or suggest all the features recited in rejected claims.

As claimed in the amended claim 1, the claimed invention relates to a transaction method between a client and a terminal, wherein the terminal is connected to a service center. Transaction data is transmitted, ***prior to*** communicating with the service center about the underlying transaction, between the customer's identification element in the mobile radio telephone and the terminal via a contactless interface. The terminal checks the authorization of the customer ***before*** a transaction document is transmitted to the service center via a public switched telephone network. The transaction document is sent to the service center ***only when*** the identification element of the customer is successfully verified. Therefore, in our invention, the authorization takes place before the terminal makes contact with the service center. According to the amended claim 1, the communication between the terminal and the

service center does not occur unless the check of the authorization of the customer is successful. The authorization check is performed using authorization data stored in the terminal and such authorization data can be updated via the public switched telephone network.

Applicants respectfully submit that Vazvan merely teaches a mobile radio telephone to be used as a wallet to perform transactions including recharging the wallet and communicating with a seller's POS for purchases. Vazvan fails to disclose, teach, or fairly suggest a transaction method between a customer and a terminal connecting to a service center, where the terminal checks, ***prior to*** sending a transaction voucher to the server, the authorization of the customer by communicating with the customer via a contact-free interface. The terminal transmits a transaction document to the service center ***only when*** the authorization of the customer is successfully performed. In addition, as correctly pointed out by the Examiner, Vazvan does not teach a transaction method where a SIM card is used to connect to a mobile radio telephone. Therefore, Vazvan does not disclose, teach, or suggest the features as claimed in amended claim 1.

Vatanen does not remedy the deficiencies of Vazvan. Vatanen discloses a SIM card that can be connected to a mobile phone for performing payment transactions. There is no entity in Vatanen's teaching corresponds to the terminal in the claimed invention. In addition, the access right of a SIM card holder (or a user) to certain services is authorized by a corresponding service provider. Therefore, Vatanen fails to disclose, teach, or fairly suggest a transaction method between a customer and a terminal connecting to a service center, where the terminal checks, ***prior to*** sending a transaction voucher to the server, the authorization of the customer by communicating with the customer via a contact-free interface. The terminal transmits a transaction document to the service center ***only when*** the authorization of the customer is successfully performed. Therefore, Vazvan and Vatanen fail to disclose, teach, or

suggest the features discussed above, as recited in claim 1. It is not obvious for one with ordinary skill in the art to devise the claimed transaction method from the method disclosed by Vazvan and Vatanen.

Pitroda does not remedy the deficiencies of Vazvan and Vatanen. Pitroda teaches a system wherein a communication interface unit (CIU) (terminal) receives client information (such as name and account number) from a universal electronic transaction card (UET) (identification element) (see column 16, lines 37-41). The CIU, upon receiving the client information, contacts a server (e.g., a financial institution such as American Express service) and transmits transaction-specific information and CIU identification information, together with the previously received client information, to the server (column 16, lines 42-47). When the server receives the transaction-specific information, the CIU identification information, and the client information, the server performs credit check and sends an authorization number to the CIU (column 16, lines 50-52). When the CIU receives the authorization number from the server, the CIU requests the client to authorize the transaction (column 16, lines 54-56).

According to Pitroda's transaction method, the information flow is (1) from the UET to the CIU (i.e., from identification element to the terminal), (2) from the CIU to the server (i.e., from the terminal to the service center), (3) from the server to the CIU (i.e., from the service center back to the terminal), (4) from the CIU to the client (i.e., from the terminal to the customer), (5) and from the client to the CIU (e.g., customer's authorization). However, according to the claimed invention, the information flow is (a) from the identification element to the terminal (i.e., customer information, amount, etc.), (b) authorization of the customer in the terminal (i.e., checking performed by the terminal), (c) from the terminal to the service center (i.e., transaction document). The flow in Pitroda (from (1) to (5) above) and the flow in the claimed invention (from (a) to (c) above) are obviously different. Therefore, the

transaction method according to the flow in Pitroda is different from the claimed transaction method.

Pitroda does not teach or fairly suggest a transaction method in which communication between the CIU and the server is subject to a ***prior*** authorization check conducted between the CIU and the UET. In the claimed invention, the authorization of the customer is performed by the terminal (instead of by the service center) and a transaction document is transmitted to the service center only when the authorization check is successful. Such a prior check reduces the risk of transmitting erroneous information to the service center. Necessary corrections can be made between the customer and the terminal without any involvement of the service center. Furthermore, Pitroda fails to teach or fairly suggest that the identification element connects to the terminal via a contactless interface.

In a wireless (contactless) communication scenario, authorization check at the terminal provides a preventive measure against data transmission errors caused by inteference and/or against mistaken customer identification due to simultaneous transmisstion from multiple identification elements. However, such authorization check does not benefit a contact-based system, as what is taught by Pitroda. Therefore, there is no motivation for Pitroda to fairly suggest or teach a transaction method with authorization check prior to sending a transaction document to the service center. Therefore, Vazvan and Vatanen in view of Pitroda fail to disclose, teach, or suggest at least the features discussed above, as recited in claim 1.

O'Mahony et al. do not remedy the discussed deficiencies. In describing various electronic payment systems, O'Mahony et al. disclose that information (e.g., a voucher) transmitted between two entities may be selectively encoded within a same data transmission. That is, some pieces of information may be encoded and some may not. Although O'Mahony et al. disclose methods related to how to encode information, they fail to disclose,

teach, or suggest, in view of Pitroda, Vazvan, and Vatanen a transaction method between a customer and a terminal connecting to a service center, where the terminal checks, ***prior to*** sending a transaction document to the service center, the authorization of the customer by communicating with the customer via a contact-free interface. The terminal transmits the transaction document to the service center ***only when*** the authorization of the customer is successfully performed.

Therefore, Applicants respectfully submit that Vazvan and Vatanen in view of Pitroda and O'Mahony fail to disclose, suggest or teach at least the features discussed above, whether individually or in combination, as recited in the amended claim 1. Therefore, the Applicants respectfully request that the rejection of claim 1 under §103(a) be withdrawn.

Claims 2-12, 15-19, 21, and 23-26 depend from claim 1. Consequently, claims 2-12, 15-19, 21, and 23-26 are patentable at least for the reasons stated above with respect to claim 1 and for the addition features recited therein. Therefore, the Applicants respectfully request that the rejection of claims 2-12, 15-19, 21, and 23-26 under §103(a) be withdrawn.

In Section 11 of the Office Action, claims 13 and 14 are rejected under 35 U.S.C. §103(a) as being unpatentable over Vazvan and Vatanen in view of Pitroda and O'Mahony et al. as applied to claim 1 and further in view of Francini et al. The rejection is respectfully traversed. The combination of Vazvan, Vatanen, Pitroda, O'Mahony, and Francini et al. fails to teach or suggest all the features recited in rejected claims.

As stated above, the combination of Vazvan, Vatanen, Pitroda, and O'Mahony et al. fails to teach or suggest all the features recited in claim 1. Francini does not remedy the discussed deficiencies. Appilicant respectifully submits that Francini et al. merely teach a transaction card with a magnetic stripe emulator adapted for use with transaction terminals that include a sensor for reading a magnetic stripe. Francini et al. fail to disclose, teach, or fairly suggest a transaction method between a customer and a terminal connecting to a service

center, where the terminal checks, ***prior to*** sending a transaction document to the service center, the authorization of the customer by communicating with the customer via a contact-free interface. The terminal transmits the transaction document to the service center ***only when*** the authorization of the customer is successfully performed. Therefore, Vazvan and Vatanen in view of Pitroda and O'Mahony et al. as applied to claim 1 and further in view of Francini fail to disclose, teach, or suggest at least the features discussed above, as recited in claim 1.

Claims 13 and 14 depend from claim 1. Consequently, claims 13 and 14 are patentable at least for the reasons stated above with respect to claim 1 and for the addition features recited therein. Therefore, the Applicants respectfully request that the rejection of claims 13 and 14 under 35 U.S.C. §103(a) be withdrawn.

In Section 12 of the Office Action, claim 20 is rejected 35 U.S.C. §103(a) as being unpatentable over Vazvan and Vatanen in view of Pitroda and O'Mahony et al. as applied to claim 1 and further in view of Yacobi (U.S. Patent No. 5,878,138). The rejection is respectfully traversed. The combination of Vazvan, Vatanen, Pitroda, O'Mahony, and Yacobi fails to teach or suggest all the features recited in the rejected claim.

As stated above, the combination of Vazvan, Vatanen, Pitroda, and O'Mahony et al. fails to teach or suggest all the features recited in claim 1. Yacobi does not remedy the discussed deficiencies. Yacobi merely teaches a combined usage of symmetrical and asymmetrical encryption for transmission of monetary information wherein the session key (symmetrical) is encrypted with the recipient's public key (asymmetrical). Yacobi does not disclose, teach, or fairly suggest a transaction method between a customer and a terminal connecting to a service center, where the terminal checks, ***prior to*** sending a transaction document to the service center, the authorization of the customer by communicating with the customer via a contact-free interface. The terminal transmits the transaction document to the

service center ***only when*** the authorization of the customer is successfully performed. Therefore, Vazvan and Vatanen in view of Pitroda and O'Mahony et al. as applied to claim 1 and further in view of Yacobi fail to disclose, teach, or suggest at least the features discussed above, as recited in claim 1.

Claim 20 depends from claim 1. Consequently, claim 20 is patentable at least for the reasons stated above with respect to claim 1 and for the addition features recited therein. Therefore, the Applicants respectfully request that the rejection of claim 20 under 35 U.S.C. §103(a) be withdrawn.

Attached hereto as an Appendix captioned **"Version with markings to show changes made"** is a marked-up version of the changes made to the claims by the current amendment.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance and a notice to that effect is earnestly solicited.

Respectfully submitted,

PILLSBURY WINTHROP LLP

By

Dale Lazar
Reg. No. 28872
Tel. No.: (703) 905-2126
Fax No.: (703) 905-2500

DSL/QCH

1600 Tysons Boulevard
McLean, Virginia
U.S.A. 22102
(703) 905-2000

APPENDIX

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Page 7, delete the whole paragraph starting in line 29, and replace it with the following paragraph.

The terminal 2' in this case, however, is a computer, which is preferably connected to a network[, for example in] such as the Internet or an Intranet. Various pieces of information or offers, for example, product offers, can be [offered] presented, for [example] instance with a suitable menu on the screen of the computer 2'. The customer can control this computer with his mobile device. For example, he can control the position of the cursor in a menu of products or information offered for sale by actuating the cursor movement keys on the keyboard 11 of his mobile telephone. The cursor movement instructions are transmitted via the contactless interface 101, 20 to the computer 2'. The user actuates a confirmation key, for example the key # on his keyboard, in order to confirm the selected menu option, for example to order a product.

Page 12, delete the whole paragraph starting in line 19, and replace it with the following new paragraph.

If this condition is not verified in step 240, [probably] it may be inferred that an unauthorized reloading process [was] probably has been carried out[,]. In this case, [and] the [method goes on] transaction process proceeds to step 241. Distinguished here is whether the falsification has been [carried out] attributed by the terminal or by the customer. If the customer is responsible, [he] the customer is entered [on] into a black list in step 242. A customer blocking document is preferably generated and sent to the mobile radio telephone 1, 10 of the customer in order to set the blocking flag and to disable the identification module associated with the customer. [this system, as well as] The customer blocking document may also be sent to all terminals or at least [all] the terminals located in a predefined geographical

area in order to enter this particular customer into the black list of [that] those terminals. If, on the other hand, the problem was caused by the terminal, The server in this case enters the [this] terminal [is entered] into a terminal black list in step 243. In addition, a terminal blocking document may be generated and sent to the terminal to disable the terminal in future transactions.

IN THE CLAIMS:

Please amend the following claims:

1. (Amended) A [F]financial transaction method between a customer and a terminal, said customer being equipped with a mobile radio telephone which can be used in a mobile radio network, said mobile radio telephone comprising a mobile device and a removable identification module, in which at least a customer identification and a monetary amount can be stored, said monetary amount being able to be reloaded [with the aid of] through secured reloading documents from a service center, [which] wherein said reloading documents are transmitted by means of digital messages via said mobile radio network, said method comprising:

transmitting, from said identification module of said mobile radio telephone, said customer identification, via a contactless interface between said identification module and said terminal, to a contactless transceiver of said terminal[,];

checking, by said terminal upon receiving said customer identification [in said terminal], authorization of said customer[,] identified by means of said transmitted customer identification[,] to carry out a financial transaction, wherein said checking tak[ing]es place with authorization data [which are transmitted to] stored in said terminal and periodically updated via a public switched telephone network[,];

transmitting, from said identification module of said mobile radio telephone, an electronic transaction amount to said terminal via said contactless interface[,];

charging the stored monetary amount [depending upon] based on said [the] transmitted transaction amount[,];

preparing, in said terminal, a transaction document, which contains said customer identification, a terminal identification as well as an indication of said transaction amount[,];

electronically signing [of] said transaction document by said terminal[,];

transmitting, upon successful checking authorization of said customer, said transaction document to the service center via said public switched telephone network[,];

checking, by said service center, [the] said electronic signature of said terminal [in said service center,]; and

paying into an account of said terminal, if [the] said electronic signature corresponds to an authorized terminal.

2. (Amended) The [T]transaction method according to claim 1, wherein said service center operates a control account for [each] said customer, wherein said control account stores [in which is stored] the value of said monetary amount that is also stored in said identification module and is[, this control account being] updated [during] when said [each reloading of said] monetary amount is reloaded and when said [during reception of] transaction document[s] is received.

3. (Amended) The [T]transaction method according to claim 2, wherein said transaction document[s are conducted] is directed to said service center by a clearing unit.

4. (Amended) The [T]transaction method according to claim 1, wherein [the] data transmitted from said mobile radio telephone to said terminal via said contactless interface [are] is provided with an electronic signature of said identification module.

5. (Amended) The [T]transaction method according to claim 4, wherein said electronic signature of said identification module is checked in said terminal.

6. (Amended) The [T]transaction method according to claim 4, wherein said electronic signature of said identification module is passed on to said service center by said terminal and is checked by said service center.

7. (Amended) The [T]transaction method according to claim 1, wherein said transaction document[s] can be transmitted in a batch mode to said service center via said public switched telephone network.

8. (Amended) The [T]transaction method according to claim 1, wherein said terminal[s] contains a customer black list, which can be updated by said service center via said public switched telephone network[,] and through which [and wherein] the transaction is interrupted if the received customer identification is [contained] included in [this] said

customer black list.

9. (Amended) The [T]transaction method according to claim 1, wherein said service center can disable said identification module [with the aid] by means of a customer blocking document[s] transmitted via said mobile radio network.

10. (Amended) The [T]transaction method according to claim 1, wherein said service center can disable [the] said terminal[s with the aid] by means of a terminal blocking document[s] transmitted via said public switched telephone network.

11. (Amended) The [T]transaction method according to claim 1, wherein said identification module is a subscriber identity module.

12. (Amended) The [T]transaction method according to claim 2, wherein said identification module is a transponder[, and said mobile device is contained in said terminal].

13. (Amended) The [T]transaction method according to claim 1, wherein said identification module communicates with said terminal via an integrated inductance in said identification module.

14. (Amended) The [T]transaction method according to claim 1, wherein said identification module communicates with said terminal [with the aid] by means of an inductance integrated into said mobile device.

15. (Amended) The [T]transaction method according to claim 1, wherein said identification module communicates with said terminal [with the aid] by means of an infrared transceiver integrated into said mobile device.

16. (Amended) The [T]transaction method according to claim 1, wherein at least [certain] a portion of data, transmitted between said terminal and said identification module via said contactless interface, is encrypted and/or signed.

17. (Amended) The [T]transaction method according to claim 1, wherein said transaction document is encrypted.

18. (Amended) The [T]transaction method according to claim 17, wherein said transaction document[s are] is not decrypted during the transmission.

19. (Amended) The [T]transaction method according to claim 17, wherein data elements[, which are] needed for the clearing in said clearing unit[,] are not encrypted, so that said clearing unit does not have to decrypt said transaction document[s].

20. (Amended) The [T]transaction method according to claim 1, wherein [the] said transaction document[s (90) are] is encrypted [with] using a symmetrical algorithm[, the symmetrical algorithm using] that uses a session key encrypted [with] using an asymmetrical algorithm.

21. (Amended) The [T]transaction method according to claim 1, wherein [the] said transaction document[s] transmitted via said [through the known] public [established <sic. Switched>] switched telephone network [(5) are] is certified and/or signed.

23. (Amended) The [T]transaction method according to claim 1, wherein said transaction document can be read or captured in said mobile device.

24. (Amended) The [T]transaction method according to claim 1, wherein said service center stores a terminal black list, and wherein the [method] transaction corresponding to said transaction document is interrupted if the received terminal identification is [contained] included in said terminal black list.

25. (Amended) The [T]transaction method according to claim 1, wherein said service center stores a customer black list, and wherein the [method] transaction corresponding to said transaction document is interrupted if said customer identification is [contained] included in said customer black list.

26. (Amended) The [T]transaction method according to claim 1, wherein said identification module [element contains] includes [a stack with] data recording [about] transactions [already] that have been carried out, and wherein said service center can access said data [can be called up by said service center].

End Appendix